

NORWICH UNIVERSITY

Risk Assessment & Risk Management

CSH5 Chapter 62
Risk Assessment and Risk Management
Robert V. Jacobsen

1


Copyright©2013 M. E. Kabay. All rights reserved.


NORWICH UNIVERSITY

Topics*

- Definitions
- Objectives of Risk Assessment
- Limits of Questionnaires
- A Model of Risk
- Risk Mitigation
- Risk Assessment Techniques

Students should note that this Quantitative Risk Management approach is strongly rejected by many security experts, including Donn Parker in particular.





* Based on Robert Jacobson's chapter in CSH5 (Bosworth, Kabay & Whyne's Computer Security Handbook, 5th edition – Wiley, 2009) with additions by M. E. Kabay

2


Copyright©2013 M. E. Kabay. All rights reserved.

Definitions




NORWICH UNIVERSITY

- Risk: *possibility of suffering harm or loss*
- Risk Management
 - ❑ Risk assessment
 - ❑ Risk mitigation
 - ❑ Security management
 - ❑ Security auditing



Feedback loops

- Feedback ensures corrective actions back into process – *continuous process improvement*
- *Security is a process, not a state**

* Attributed to Bruce Schneier


3

Copyright©2013 M. E. Kabay. All rights reserved.

Objectives of Quantitative Risk Assessment (QRA)


NORWICH UNIVERSITY

- Help to select subset of security measures given limitations on resources
- Every system will have unique security requirements
- Risk assessment must provide appropriate information about
 - ❑ Possible losses (costs of damage and of recovery)
 - ❑ Estimated probability* of specific events or classes of events




* Fundamental difficulty for QRA


4

Copyright©2013 M. E. Kabay. All rights reserved.

A Model of Risk


NORWICH UNIVERSITY


- Fundamental Risk Model
- Two Inconsequential Risk Classes
- Two Significant Risk Classes
- Real-World Risks & the ALE



5

Copyright©2013 M. E. Kabay. All rights reserved.

Fundamental Risk Model


NORWICH UNIVERSITY

"Jacobson's Window"

		Consequences	
		Low	High
Occurrences	Low		
	High		

6

Copyright©2013 M. E. Kabay. All rights reserved.

Two Inconsequential Risk Classes

		Consequences	
		Low	High
Occurrences	Low	Don't care	
	High		Doesn't happen

7

Two Significant Risk Classes

		Consequences	
		Low	High
Occurrences	Low		Major fire, long power outage, flooding, cash fraud,
	High	Power transient, minor sw bug, keystroke error,	

8


Real-World Risks & the ALE

➤ To compare risks, we use the *annualized loss expectancy* (ALE):

$$E(x) = \sum_i p_i c_i$$

➤ Where

- ☐ $E(x)$ = ALE of strategy x
- ☐ p_i = probability of occurrence i
- ☐ c_i = cost of occurrence i
- ☐ Σ = add up the products




9

Example of ALE Calculation

Keystroke errors (Jacobson's example with slight modifications)

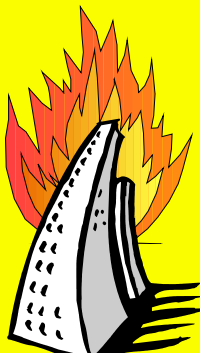
- 100 errors per operator per hour
- 100 operators
- 2,000 hours per operator per year
- = 20,000,000 errors per year
- Detection rate 99.9% at no cost
- Thus $p = 0.001$ failure rate of missed errors
- Errors corrected later @ \$1 each
- So $E(X) = 0.001 * 20,000,000 * \$1 = \$20,000$



10

Another ALE Calculation


- Major fire (also Jacobson's example)
- Probability "p" of major fire in a year = 0.0001
- Cost of major fire estimated at \$100M
- Therefore $E(x) = 0.0001 \times \$100M = 10^{-4} \times 10^8 = 10^4 = \$10,000$



11

ALE of an Insurance Policy

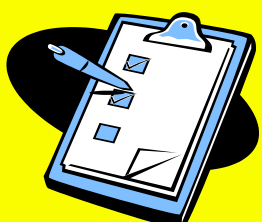
- Customer bets insurance company he will die this year (probability 0.1%)
- Bets (pays) \$750 in "premium"
- If customer dies, insurance company pays \$500,000 to beneficiary
- Insurance company bets that customer lives – keeps premium, pays nothing.
 - ☐ $p_1 = 0.001$ $c_1 = -\$500,000$ (a gain to widow and a loss to the insurance company)
 - ☐ $p_2 = 0.999$ $c_2 = +\$750$ (a loss to family and a gain to the insurance company)
- $E(x) = \sum p_i c_i = 0.001 \times -\$500,000 + 0.999 \times +\$750 = +\$249.25$ (a loss to the family and a gain to the company)



12

Risk Mitigation

- Difficulties Applying ALE Estimates
- Risk Managers' Goals
- Mitigating Infrequent Risks
- Summary of Risk-Mitigation Strategies




NORWICH UNIVERSITY

13 Copyright©2013 M. E. Kabay. All rights reserved.

Difficulties Applying ALE Estimates

- Information about information assurance risks is very poor
 - ❑ Little or no mandatory reporting
 - ❑ No centralized databanks
 - ❑ Enormous variety of system configurations
 - ❑ Therefore no actuarial statistics
- Jacobson's 30-Year Law
 - ❑ People dismiss risks not personally experienced in last 30 years
- Kabay's Paradox of Security
 - ❑ The better the security, the less direct evidence there is to support security measures in a specific organization
 - ❑ UNLESS you have METRICS



NORWICH UNIVERSITY

14 Copyright©2013 M. E. Kabay. All rights reserved.

Risk Managers' Goals

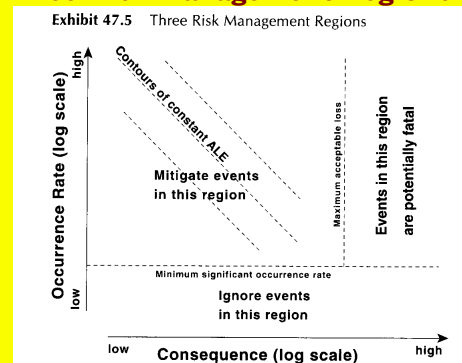
- Imagine wide range of risks
- Try to estimate consequences / costs
- Attempt to determine probabilities
- Identify risk-mitigation strategies and their costs
- Compute ALEs to estimate appropriate return on investment (ROI)
 - ❑ Generally focus on loss-avoidance
 - ❑ However, some loss-avoidance can reduce costs to such a point as to provide overall increase in profitability
 - ❑ Also consider secondary effects such as improved customer relations, marketability, visibility in competitive marketplace....

NORWICH UNIVERSITY

15 Copyright©2013 M. E. Kabay. All rights reserved.

Three Risk-Management Regions

Exhibit 47.5 Three Risk Management Regions




NORWICH UNIVERSITY

16 © Copyright 2001 International Security Technology, Inc.

Where ROI-Based Risk Mitigation is Effective

- Works well for high-probability, low-cost risk exposures
 - ❑ Realistic appraisal by managers
 - ❑ Data are credible
- Does not work well for low-probability, high-cost risk exposures
 - ❑ Upper management rarely understand implications of information technology risks
 - ❑ "Who would have thought that...." is common reaction by upper management



NORWICH UNIVERSITY

17 Copyright©2013 M. E. Kabay. All rights reserved.

Four Reasons for Adopting a Mitigation Strategy

1. Required by law or regulations
2. Cost trivial but significantly lowers probability of harm
3. Addresses low-probability, high-cost event with unacceptable SOL (single-occurrence loss); e.g., consequence that wipes out org.
4. Cost of mitigation is more than offset by expected reduction in ALE (i.e., positive ROI overall compared with doing nothing)





NORWICH UNIVERSITY

18 Copyright©2013 M. E. Kabay. All rights reserved.

Mitigating Infrequent Risks

- Reduce magnitude of high SOLs*
 - ❑ Transfer risks using insurance
 - ❑ Disperse risk exposure (e.g., multiple ops centers)
 - ❑ Reduce vulnerability (e.g., BCP)
- Mitigation selection process
 - ❑ Choose low-cost measures
 - ❑ Ignore low risks
 - ❑ Use insurance



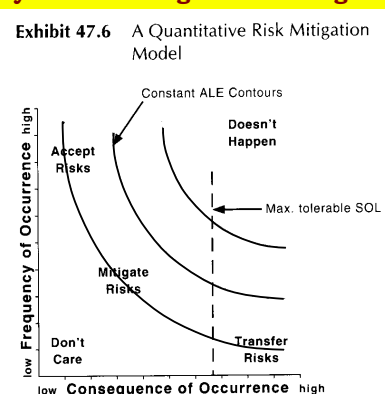
* Single-occurrence losses

19

Copyright©2013 M. E. Kabay. All rights reserved.

Summary of Risk-Mitigation Strategies (1)

Exhibit 47.6 A Quantitative Risk Mitigation Model




low Frequency of Occurrence high

low Consequence of Occurrence high

20

Summary of Risk-Mitigation Strategies (2)

- IT staff may be unable to reduce ALE of high-probability/low-consequence risks
- Midrange risks can be handled using mitigation measures chosen by evaluating their ROI using ALE calculations
- Low-probability/high-cost risks involve evaluations of SOLs and mitigation measures to reduce probabilities further or reduce costs through planning and preparation
- Ideally, risk management should be
 - ❑ Performed by experts
 - ❑ Independent of IT management
 - ❑ Reported to senior management directly

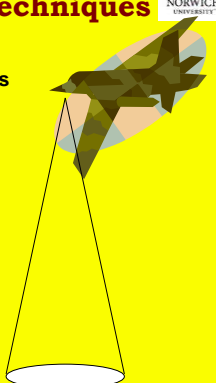


21

Copyright©2013 M. E. Kabay. All rights reserved.

Risk Assessment Techniques

- Aggregating Threats and Loss Potentials
- Basic Risk-Assessment Algorithms
- Loss-Potential Risk-Event Parameters
- Risk Event Parameters
- Vulnerability Factors, ALE, SOL Estimates
- Sensitivity Testing
- Selecting Risk-Mitigation Measures



22

Copyright©2013 M. E. Kabay. All rights reserved.


Aggregating Threats and Loss Potentials

- Calculations of ALE can be increased in precision using aggregation of individual ALEs for specific components of systems
 - ❑ E.g., if manufacturers provide failure rates for specific components (e.g., servers), these data can be helpful in estimating overall failure rates
- One useful rule: probability P of failure of a system with independent units "i" where each has probability p_i of failing is

$$P = 1 - \prod(1-p_i) \text{ which reduces to}$$

$$P = 1 - (1-p)^n$$

for systems where all the units have the same p_i



23

Copyright©2013 M. E. Kabay. All rights reserved.

Loss-Potential

Loss potential can include costs of

- Property damage
- Liability
- Service interruption




24

Copyright©2013 M. E. Kabay. All rights reserved.

Risk Event Parameters

- Occurrence rate estimation
 - ❑ Rates often change after problems occur
 - ❑ Don't count events twice; e.g., if a *power failure* causes a *system crash*, be careful not to count both of these separately
 - ❑ Look for external source of actuarial data
- Outage duration affects costs
 - ❑ Service interruption increasingly important with e-commerce growing
 - ❑ EDI, Web purchases, multiple competitors....



Copyright © 2013 M. E. Kabay. All rights reserved.

Vulnerability Factors, ALE, SOL Estimates


- Validating the estimates is important
- Check all the individual data and calculations before basing decisions on math
- Look for the risk event/loss potential pairs that generate ~80% of total ALE
- Check assumptions – discuss with team members
- Look for outliers – extraordinarily large contributors – and double-check them





Copyright © 2013 M. E. Kabay. All rights reserved.

Sensitivity Testing

- Estimates of probability and costs are unlikely to be point-estimates
- Can use range estimates
 - ❑ Try high, medium and low
- If probability distributions are available, try *Monte Carlo simulation*
 - ❑ Run random trials selecting values from parameter distributions
 - ❑ Plot range of resulting ALEs to see central tendencies
 - ❑ Compute expected distributions
 - ❑ Look out for chaotic systems*



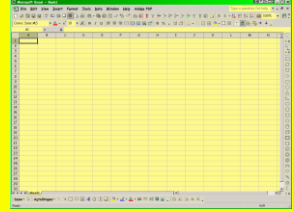

* System that is so sensitive to initial conditions that it is unpredictable



Copyright © 2013 M. E. Kabay. All rights reserved.

Selecting Risk-Mitigation Measures



- Address intolerable SOLs
- Discard mitigation with negative ROIs (but remember that insurance always has a short-term negative ROI)
- Rank measures by descending benefits, costs, ROI

Copyright © 2013 M. E. Kabay. All rights reserved.

Limits of Questionnaires


- Could a security questionnaire suffice as a risk assessment?
 - ❑ Ask people for their opinions
 - ❑ Collate the results
- Problems
 - ❑ Ambiguities in use of words (“serious”, “expensive”....
 - ❑ Many questions prompt yes/no answers but need more subtle distinctions
 - ❑ Questionnaires miss points that arise in open discussion with back-and-forth exchange of ideas
- Use Computer-Aided Consensus™
 - ❑ http://www.mekabay.com/methodology/cac_ppt.zip
 - ❑ http://www.mekabay.com/courses/academic/norwich/msia/leadership_skills_part_5_ppt.zip
 - ❑ <http://www.mekabay.com/methodology/cac.pdf>

Copyright © 2013 M. E. Kabay. All rights reserved.

Review Questions (1)

1. What are the two main components of *risk* as discussed in IA management?
2. Why can't we apply the same risk management choices to all IT systems? How come it's not like car safety?
3. What are the major problems limiting the value of questionnaires in determining IT risks in an organization?
4. What is Jacobson's Window? Draw it.
5. What are the two classes of risk that are simply irrelevant in managing risks? Explain why each of the two has no real-world significance for risk management.
6. What are the two classes of risk that are critically important in real-world risk management?



Copyright © 2013 M. E. Kabay. All rights reserved.

Review Questions (2)



7. What is the ALE for a 100-year flood (one that occurs on average once in a century) that completely destroys a \$10M building?
8. What is the ALE for a meteor strike equivalent to the C-T (Cretaceous-Tertiary) extinction event that killed off 99.9% of the dinosaurs and other living things and led to a decades-long global winter 65 million years ago? Assume that such an event has an occurrence rate of 1 per 100 million years and make reasonable estimates of the global domestic product if the entire human population were to be destroyed.
9. Calculate the Expected Value $E(x)$ for a BCP & DRP that costs \$10,000 per year, is used on average only once in a century, but saves the organization \$15M if it is actually used.

31

Copyright©2013 M. E. Kabay. All rights reserved.

DISCUSSION



32

Copyright©2013 M. E. Kabay. All rights reserved.